

**REMARKS/ARGUMENTS**

This amendment is being submitted in response to the Office Action dated February 13, 2004. Claims 1-35 are pending. Claims 1, 9, 15, 22 and 28 were amended, and claims 36 and 37 were added. Claims 1-37 remain pending.

Independent claims 1, 9, 15, 22 and 28 were amended to make clear that the indicia generating devices are divided into groups based on geographic designations, and that sets of verification keys are encrypted as a function of the geographic destinations. Independent claims 1, 11, and 19 have also been amended to make clear that both the sets of verification keys and corresponding key ID's encrypted as a function of a particular geographic designation are distributed via the network to the devices and establishments associated with that same geographic designation. Support for the amendment can be found throughout the specification and original claims (See for example pages 7 and 8). New claims 36 and 37 incorporate subject matter canceled from independent claims 15 and 22. Accordingly no new matter has been entered.

A telephone interview was held on June 16, 2004, between Examiner James Curcio, Supervisor Gilberto Barron and Attorney for Applicant. Attorney for Applicant thanks and appreciates the helpful comments and suggestions offered by Examiner Colin to facilitate allowance of the application. In the interview, the differences between Heiden (US 6,438,530) and the amended claims were discussed. Namely, Heiden fails to teach dividing the generating devices, verification keys and key IDs, and establishments that receive the media, into groups based on geographic designation, and distributing only the verification keys and key IDs for each group to the corresponding generating devices and establishments. In addition it was discussed that Heiden only teaches the use of "a

cryptographic key", rather than sets of verification keys.

The Examiner rejected claims 1, 7, 10, 16, 19, and 25 under 35 USC §102 (e) as being anticipated by US patent 6,438,530 Heiden et al. The Examiner rejected claims 3-7, 11-14, 16-21 and 24-31 under 35 USC §103 (a) as being unpatentable over Heiden. The Examiner rejected claims 8 under 35 USC §103(a) as being unpatentable over Heiden in view of US publication 20030028497A1 to Leon. Applicant respectfully disagrees.

The present invention is related to using cryptographic methods, such as asymmetric public-key cryptography, to prevent counterfeiting of the USPS information printed onto mail pieces and other items. The present invention accomplishes this by securely distributing different sets of verification keys and key IDs to corresponding groups of indicia generating devices and establishments.

Heiden, in contrast, provides a system for purchasing a book of digital stamps over the Internet. In response to a request to purchase stamps, a data center downloads the book of stamps to the PC in the form of a software module that generates the digital stamps in the PC that initiated the purchase of the book of stamps.

Heiden is similar to the prior art discussed in the background of the invention in the present application in which the keys for the generating postage are stored at a data center. Heiden explicitly states "the digital signature for the postage stamp is generated at the data center using a cryptographic key to sign at least some of the postage stamp data." (col. 7, lines 56-58). As described in the background of the present invention, maintaining possession of the cryptographic keys at a central location is disadvantageous. The data center is a single point of attack: if the data center is broken into, a perpetrator

may easily impersonate all postage generating devices in the postal system.

The present invention solves this problem by dividing postage generating devices (PDGs) into  $n$  groups corresponding to different geographic designations, and by assigning a set of set of verification keys,  $V_i$ , to each PGD group, where each verification key in the set is encrypted as a function of one the corresponding geographic designations.

Steps (a) and (b) in amended claim 1 now recite that a set of verification keys and corresponding key ID's are encrypted as a function of one of the same geographic designation as the PDG's to which the keys are assigned. In Heiden, there is no teaching or suggestion that any type of keys are grouped based on geographic designation and then assigned to corresponding groups of PC's, and establishments.

The Examiner considers Heiden's PCs as analogous to the claimed PGDs, but the Examiner fails to point out where Heiden teaches or suggest that the PCs "are divided into groups, each group corresponding to a respective geographic designation," as recited in claim 1. The Examiner cites Heiden col. 7, lines 21 -24, 27-32 and 45-55 for teaching assigning a plurality of verification keys. However, nothing in the cited passages teach or suggest that sets of verification keys are encrypted as a function of respective geographic designations, and that each set is then assigned and distributed to the device group in the same geographic designation via a network, as recited in step (a) of claim 1. Instead, Heiden teaches states that the software module generates the digital postages stamp using stamp data (col. 7, lines 21-24), but stamp data is defined as "origin zip code of the PC, denomination of the digital postage stamp and date of request, user data..., and the digital signature of the postage stamp" (col. 7, line 47). There is no mention of keys of

any kind being included in the stamp data.

Heiden does state that the software module "signs or encrypts the concatenation of the postage stamps digital signature and the addressee information using a key stored within the software module to produce a second digital signature" (col. 9, lines 45-53). Even so, this key is not encrypted by geographical designation. This key is not included in a set of keys that is assigned and distributed to the devices in the same geographic group. This key is not distributed to establishments located in that geographic designation that perform the verification. Nor is the key accompanied by a key ID that can identify the key, all as called for in steps (a)-(c) of claim 1.

With respect to step (b), the present invention uses key ID so that it can be determined during verification which verification key in the set was used to evidence the indicia. Heiden fails to teach or suggest the use of keys that identify Heiden's cryptographic key because Heiden does not teach that multiple cryptographic keys are used, or that one needs to identify which one of those keys were used to verify the indicia.

With respect to step (e) of claim 1, Heiden fails to teach or suggest that upon receiving the media at the particular establishment, the indicia on the media is verified using the key ID on the indicia and the distributed verifications keys to compute a digital signature, and the computed digital signature compared with the digital signature on the indicia. In Heiden, by contrast, the verification is performed by verification subsystem 60. Heiden fails to teach or suggest that the verification system 60 is located in geographical regions that were used to encrypt the verification keys and key IDs, that the corresponding set of verification keys are distributed to respective establishment, or that

the key ID printed on the indicia is used with the set of verification keys to verify the indicia, as claimed.

Based on the foregoing, it respectfully submitted that Heiden fails to teach or suggest independent claims 1, 9, 15, 22, 28, and 32, even when combined with the secondary references. It is respectfully submitted that a secondary reference stands or falls with a primary reference, and the secondary references fail to make up for the lack of teaching in Heiden.

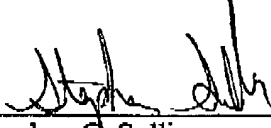
In view of the foregoing, it is submitted that claims 1, 9, 15, 22, 28 and 32 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-37 as now presented.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

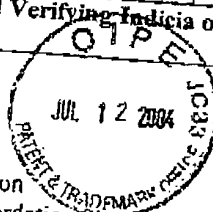
Respectfully submitted,  
SAWYER LAW GROUP LLP

July 9, 2004

Date

  
\_\_\_\_\_  
Stephen G. Sullivan  
Attorney for Applicant(s)  
Reg. No. 38,329  
(650) 493-4540

JUL 16 2004

Docket No: 1775P		Date: July 9, 2004
Serial No: 09/608,735		Filed: June 30, 2000
Inventor(s): Martin J. PAGEL		
Title: Evidencing and Verifying Indicia of Value Using Secret Key Cryptography		
<div style="text-align: center;"></div>		
<input checked="" type="checkbox"/> Transmittal	<input type="checkbox"/> Petition for Extension of Time	
<input checked="" type="checkbox"/> Amendment	<input type="checkbox"/> Part B-Issue Fee Transmittal	
<input type="checkbox"/> Response to	<input type="checkbox"/> Letter to Draftsman	
<input type="checkbox"/> Executed Declaration	<input type="checkbox"/> ___ Sheets of Formal Drawings	
<input type="checkbox"/> Assignment + Recordation Sheet	<input checked="" type="checkbox"/> Fee Payment: \$228.00	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Deposit Account (Name)	
<input type="checkbox"/> Form 1449 with ___ References	<input checked="" type="checkbox"/> Check No. 7616	

The Stamp of the USPTO Hereon Certifies Receipt of the Above